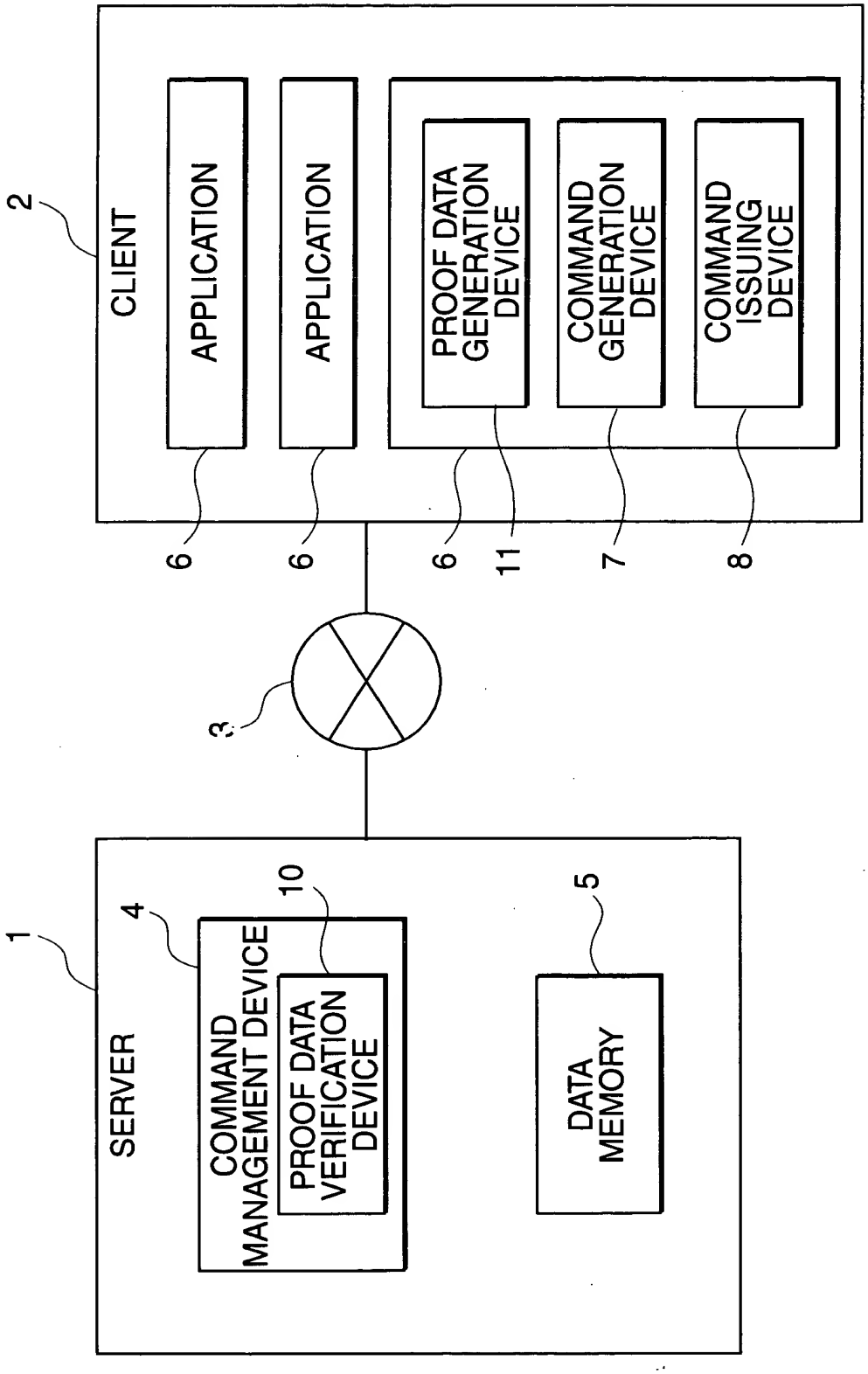
FIG.1


1
SERVER
4
COMMAND MANAGEMENT DEVICE
10
PROOF DATA VERIFICATION DEVICE
5
DATA MEMORY
3
2
CLIENT
APPLICATION
APPLICATION
PROOF DATA GENERATION DEVICE
COMMAND GENERATION DEVICE
COMMAND ISSUING DEVICE
6
6
6
11
7
8

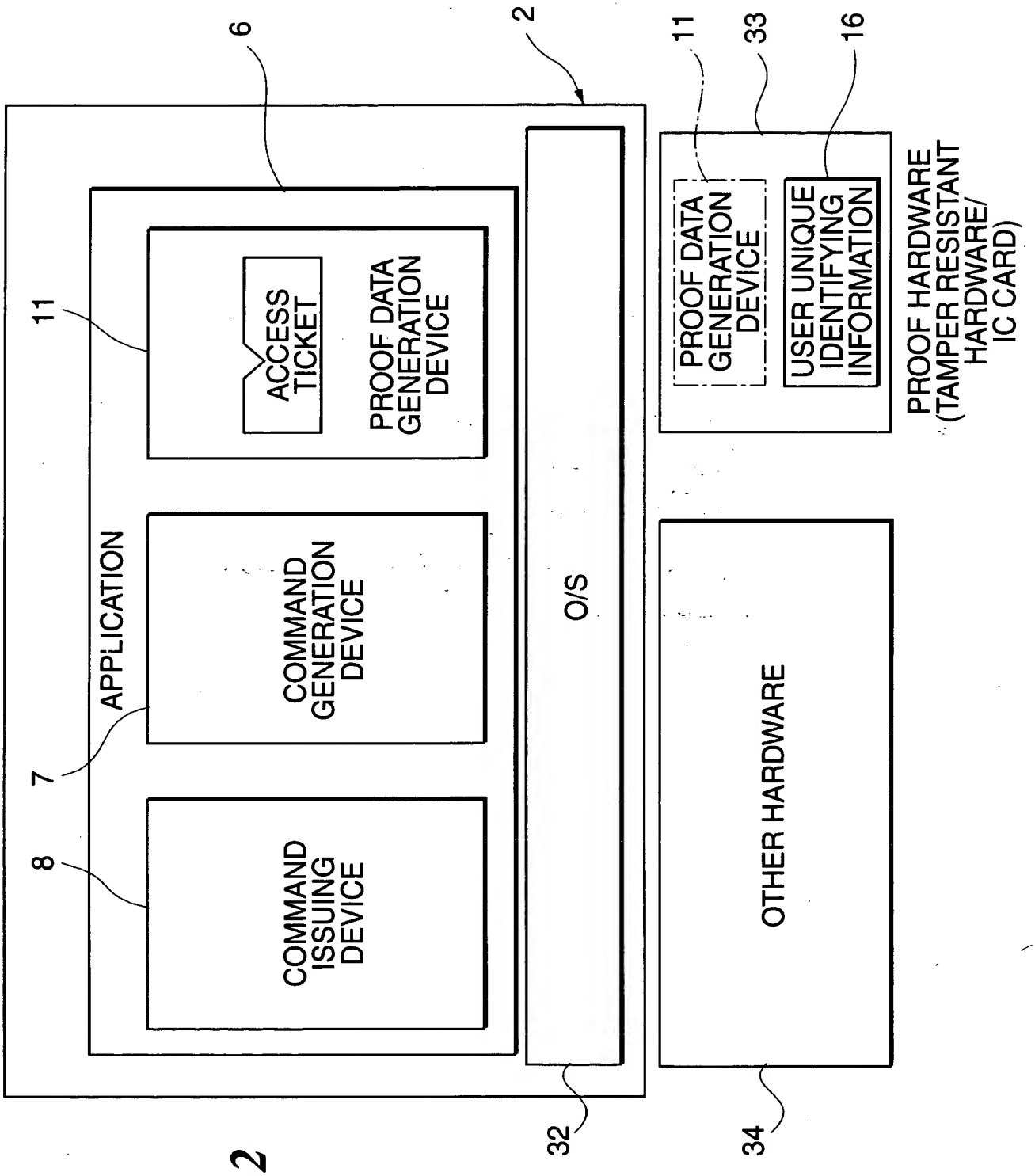

6
2
11
33
16
11
APPLICATION
ACCESS TICKET
PROOF DATA GENERATION DEVICE
COMMAND GENERATION DEVICE
O/S
PROOF DATA GENERATION DEVICE
USER UNIQUE IDENTIFYING INFORMATION
PROOF HARDWARE (TAMPER RESISTANT HARDWARE/ IC CARD)
7
8
COMMAND ISSUING DEVICE
OTHER HARDWARE
32
34

FIG.2

FIG.3

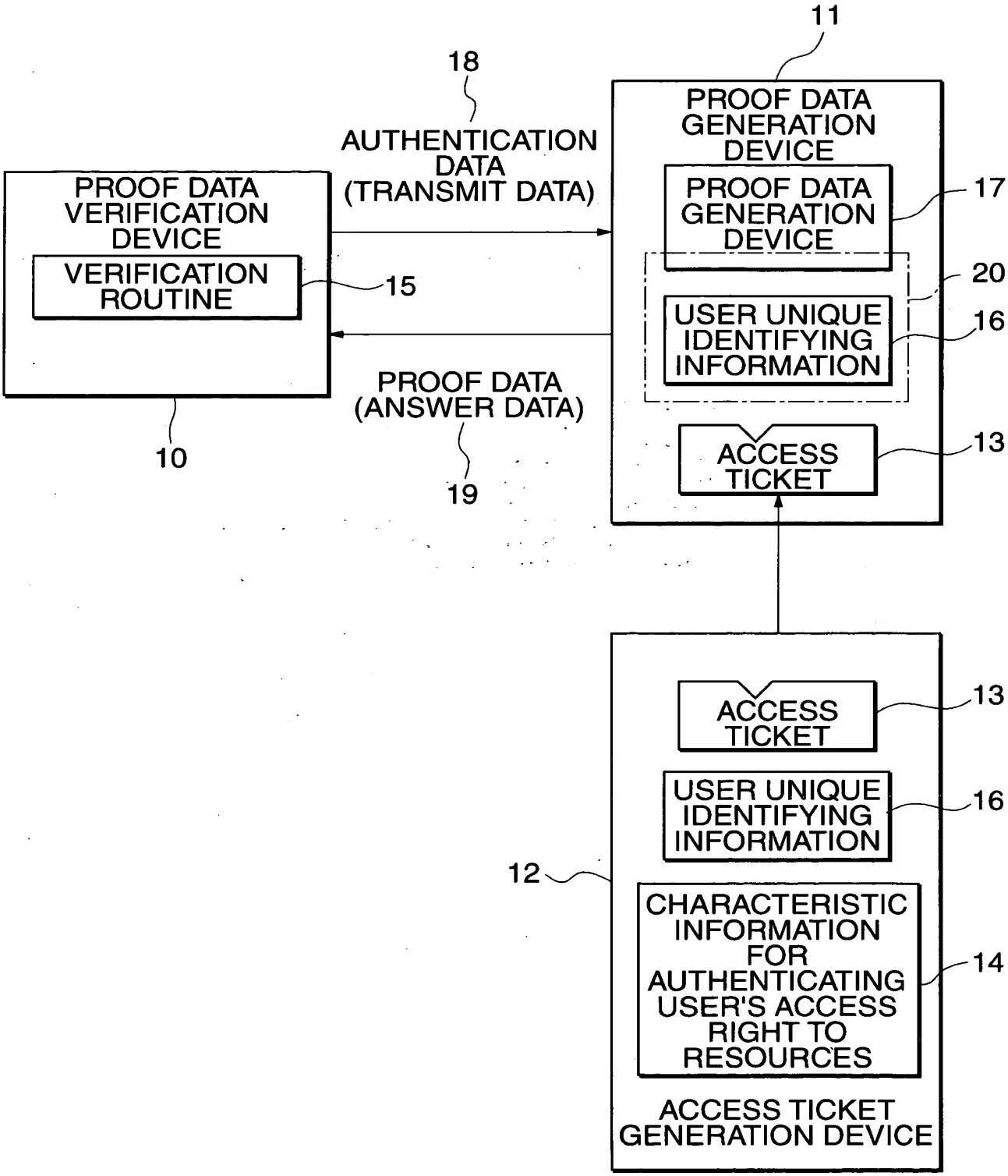

11
18
AUTHENTICATION DATA (TRANSMIT DATA)
PROOF DATA GENERATION DEVICE
PROOF DATA GENERATION DEVICE
17
PROOF DATA VERIFICATION DEVICE
VERIFICATION ROUTINE
15
20
USER UNIQUE IDENTIFYING INFORMATION
16
PROOF DATA (ANSWER DATA)
ACCESS TICKET
13
10
19
ACCESS TICKET
13
USER UNIQUE IDENTIFYING INFORMATION
16
12
CHARACTERISTIC INFORMATION FOR AUTHENTICATING USER'S ACCESS RIGHT TO RESOURCES
14
ACCESS TICKET GENERATION DEVICE

FIG.4

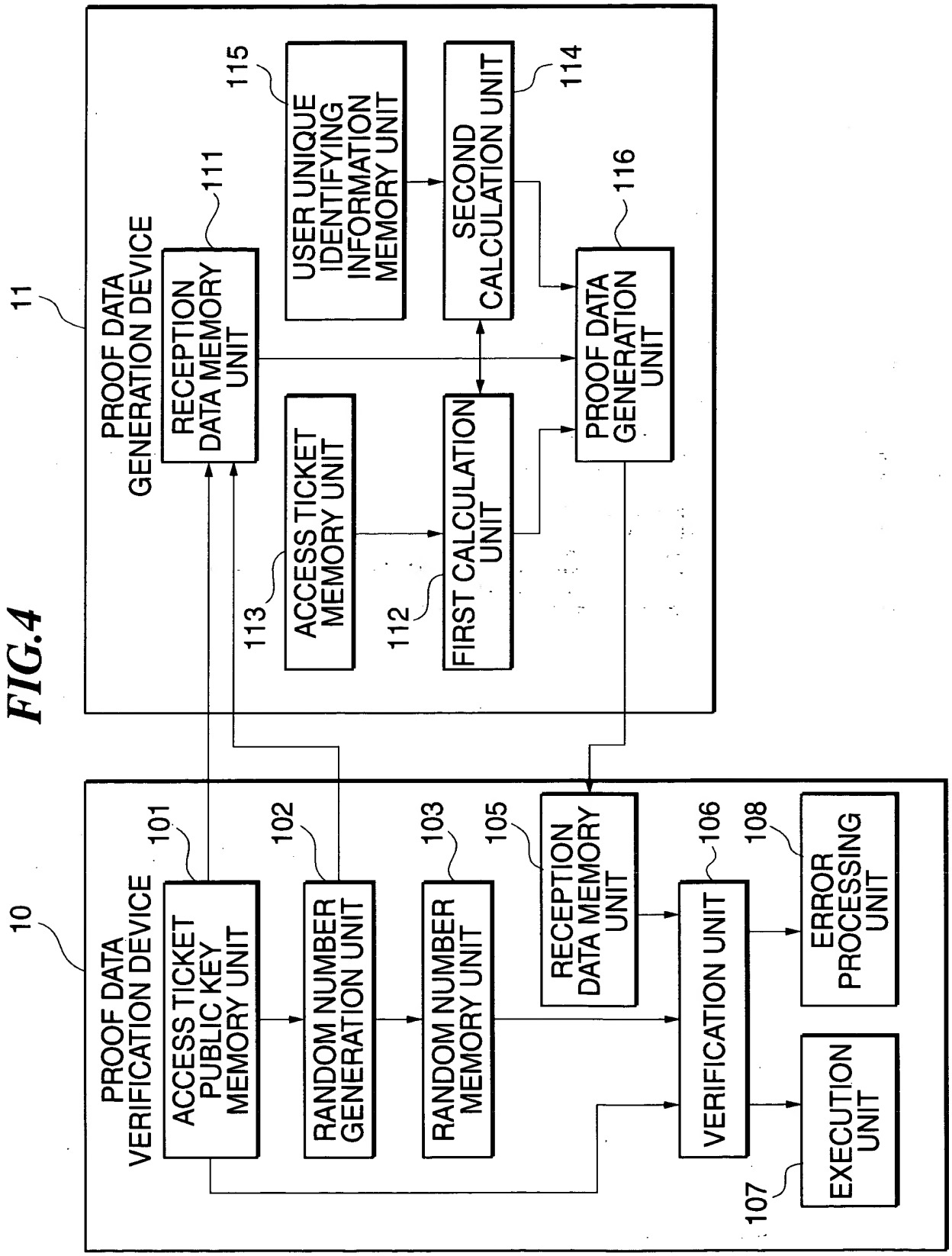

PROOF DATA VERIFICATION DEVICE
10
ACCESS TICKET PUBLIC KEY MEMORY UNIT
101
RANDOM NUMBER GENERATION UNIT
102
RANDOM NUMBER MEMORY UNIT
103
RECEPTION DATA MEMORY UNIT
105
VERIFICATION UNIT
106
ERROR PROCESSING UNIT
108
EXECUTION UNIT
107
PROOF DATA GENERATION DEVICE
11
RECEPTION DATA MEMORY UNIT
111
ACCESS TICKET MEMORY UNIT
113
FIRST CALCULATION UNIT
112
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
115
SECOND CALCULATION UNIT
114
PROOF DATA GENERATION UNIT
116

FIG.5

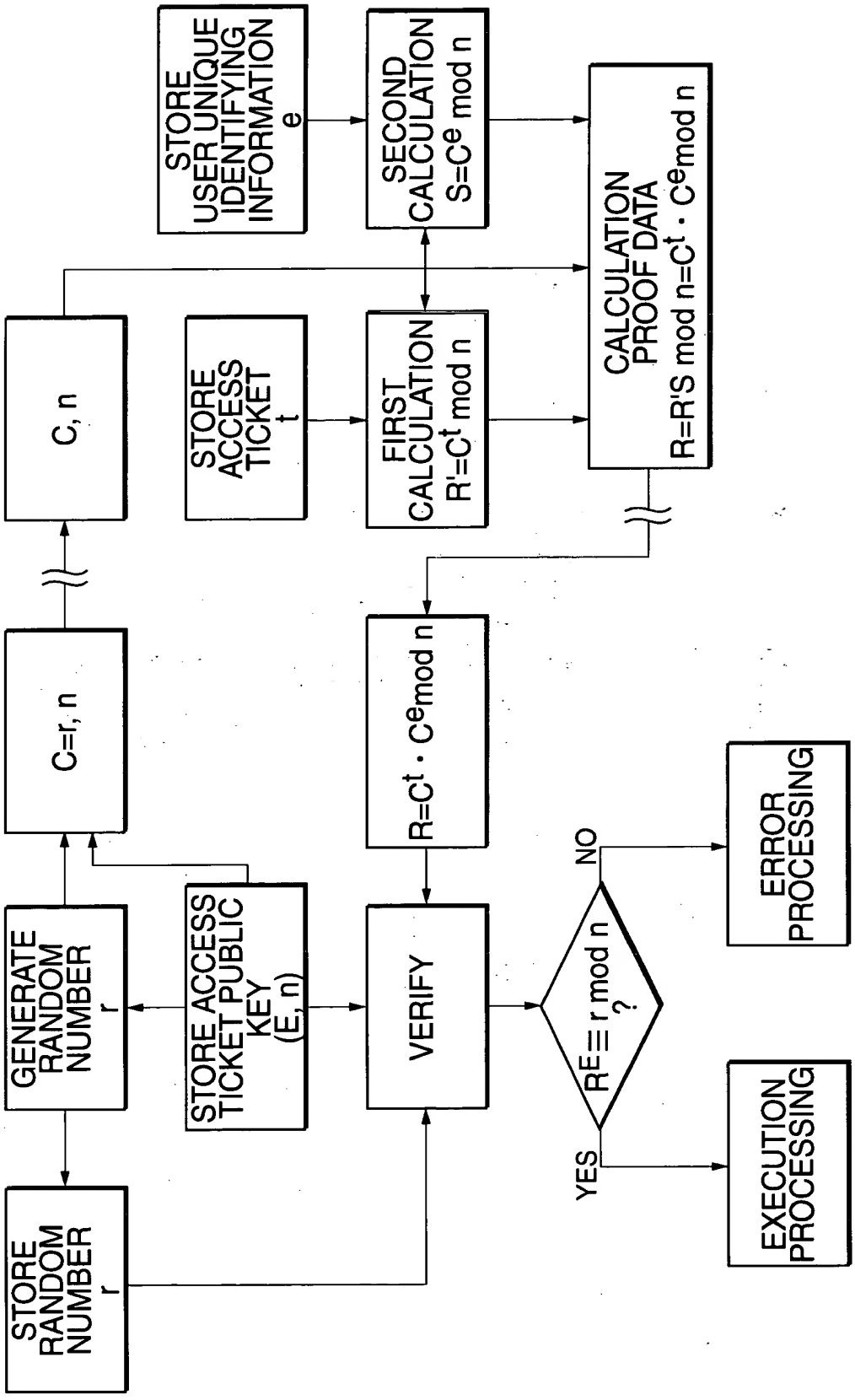

STORE USER UNIQUE IDENTIFYING INFORMATION e
SECOND CALCULATION S=C^e mod n
CALCULATION PROOF DATA R=R'S mod n=C^t · C^e mod n
C, n
STORE ACCESS TICKET t
FIRST CALCULATION R'=C^t mod n
C=r, n
R=C^t · C^e mod n
GENERATE RANDOM NUMBER r
STORE ACCESS TICKET PUBLIC KEY (E, n)
VERIFY
RE≡ r mod n ?
NO
YES
ERROR PROCESSING
EXECUTION PROCESSING
STORE RANDOM NUMBER r

FIG.6

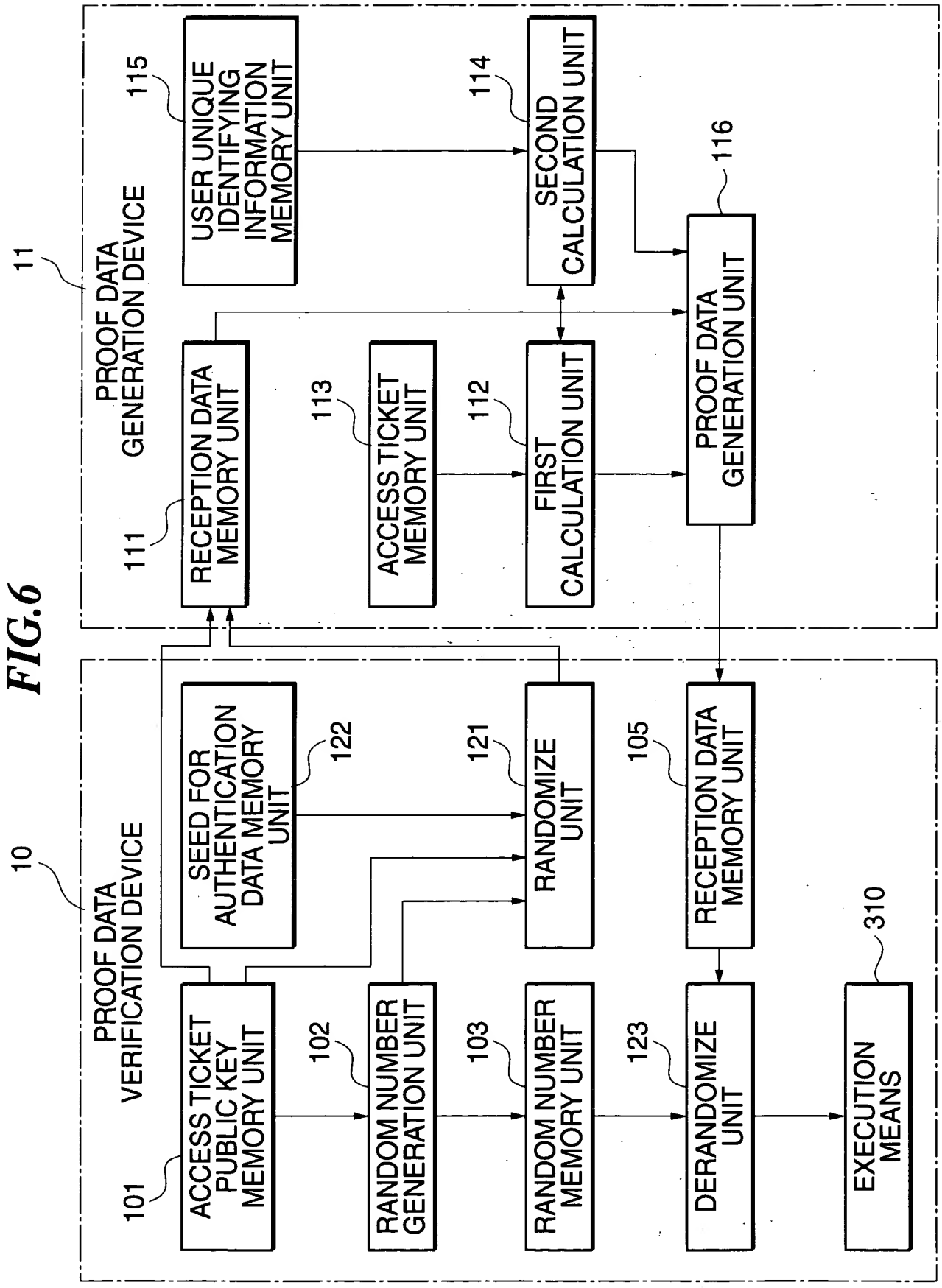

PROOF DATA VERIFICATION DEVICE
10
ACCESS TICKET PUBLIC KEY MEMORY UNIT
101
RANDOM NUMBER GENERATION UNIT
102
RANDOM NUMBER MEMORY UNIT
103
SEED FOR AUTHENTICATION DATA MEMORY UNIT
122
RANDOMIZE UNIT
121
RECEPTION DATA MEMORY UNIT
105
DERANDOMIZE UNIT
123
EXECUTION MEANS
310
PROOF DATA GENERATION DEVICE
11
RECEPTION DATA MEMORY UNIT
111
ACCESS TICKET MEMORY UNIT
113
FIRST CALCULATION UNIT
112
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
115
SECOND CALCULATION UNIT
114
PROOF DATA GENERATION UNIT
116

FIG.7

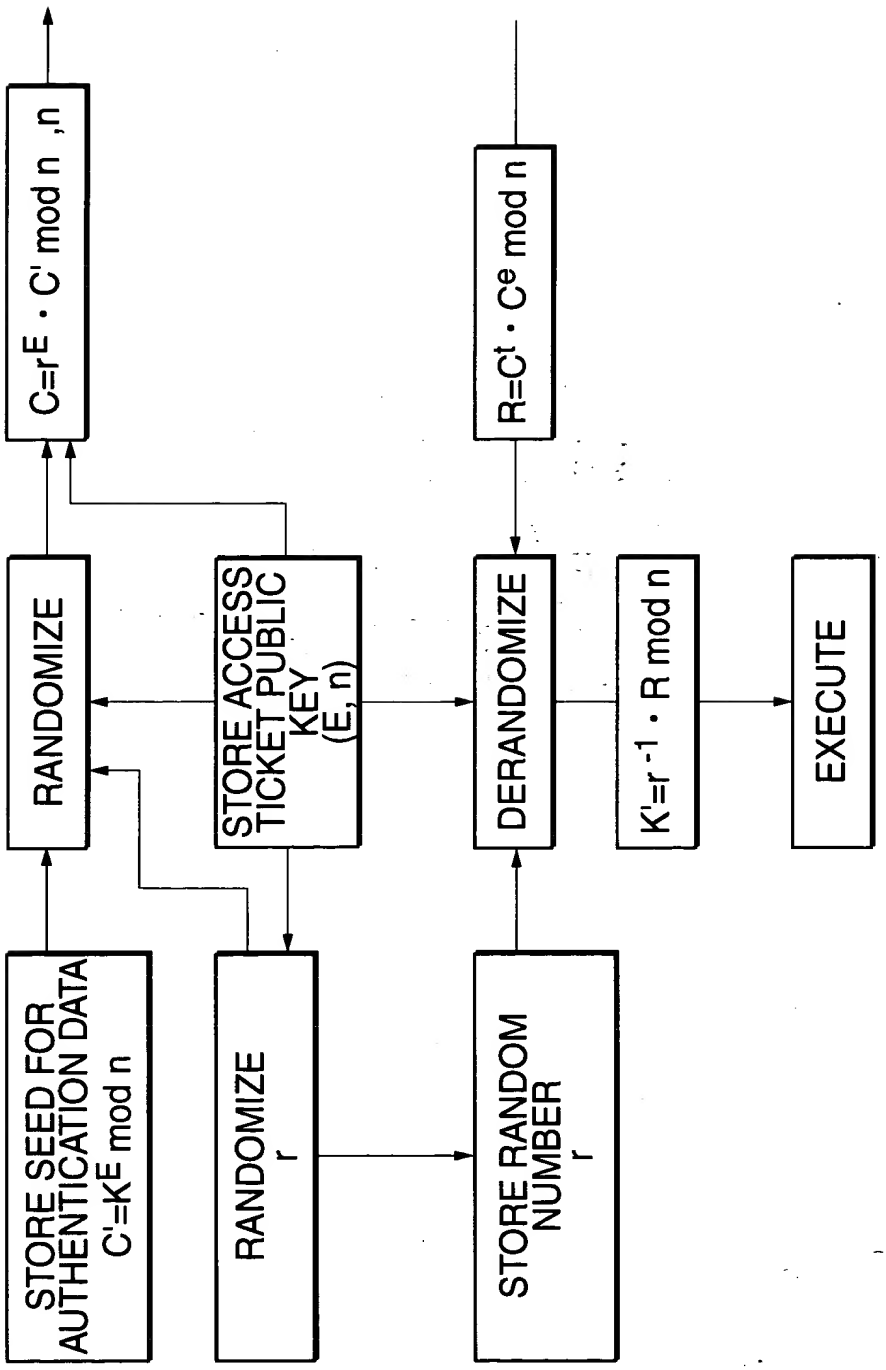

STORE SEED FOR AUTHENTICATION DATA
C'=K^E mod n
RANDOMIZE
C=r^E · C' mod n ,n
RANDOMIZE
r
STORE ACCESS TICKET PUBLIC KEY
(E, n)
STORE RANDOM NUMBER
r
DERANDOMIZE
R=C' · C^e mod n
K'=r^-1 · R mod n
EXECUTE

FIG.8

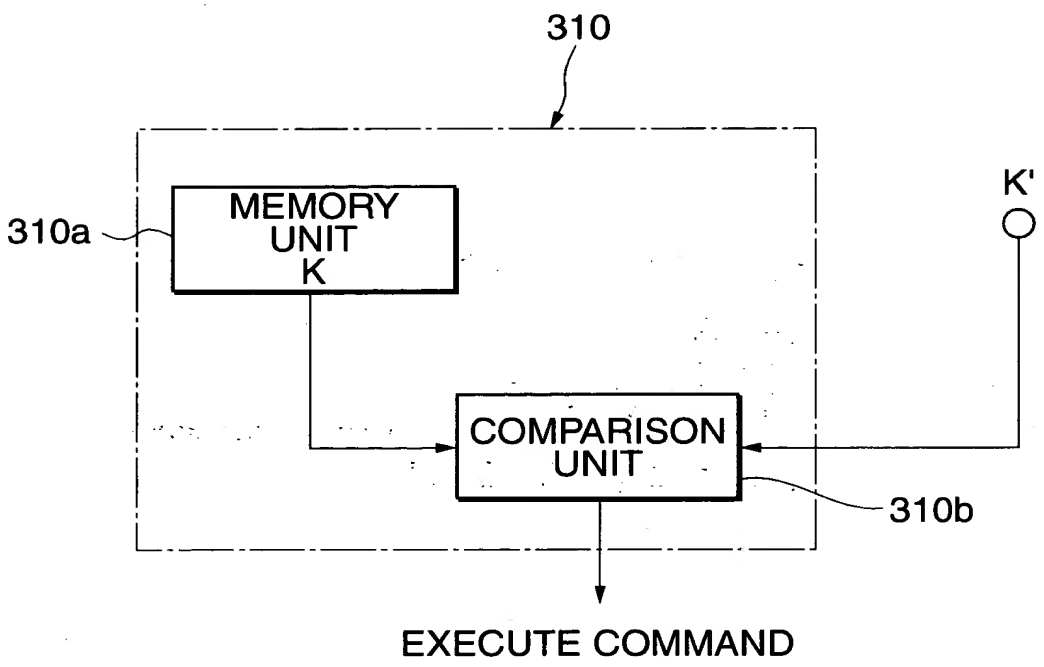

310
310a
MEMORY UNIT K
K'
COMPARISON UNIT
310b
EXECUTE COMMAND

FIG.9

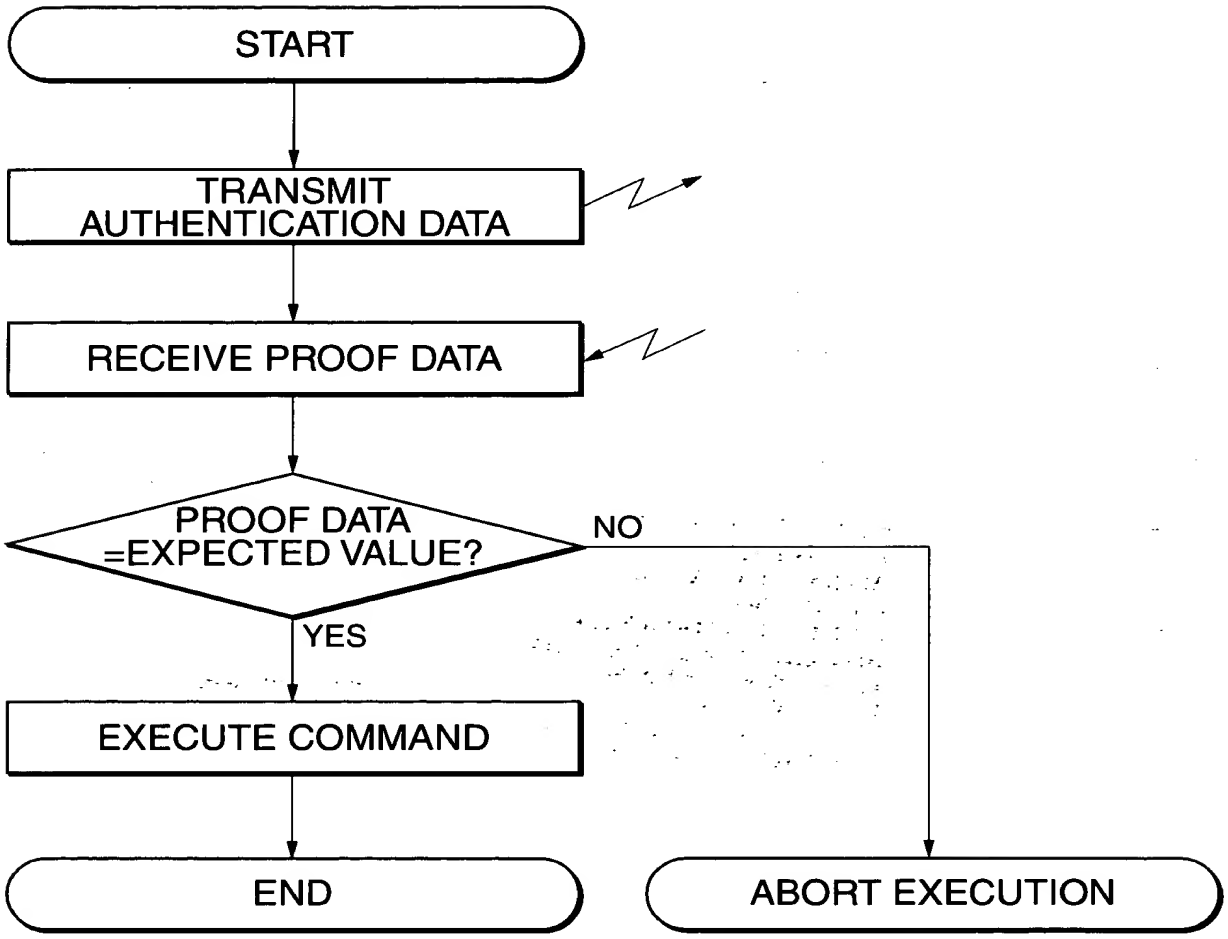

START
TRANSMIT AUTHENTICATION DATA
RECEIVE PROOF DATA
PROOF DATA =EXPECTED VALUE?
NO
YES
EXECUTE COMMAND
END
ABORT EXECUTION

FIG.10

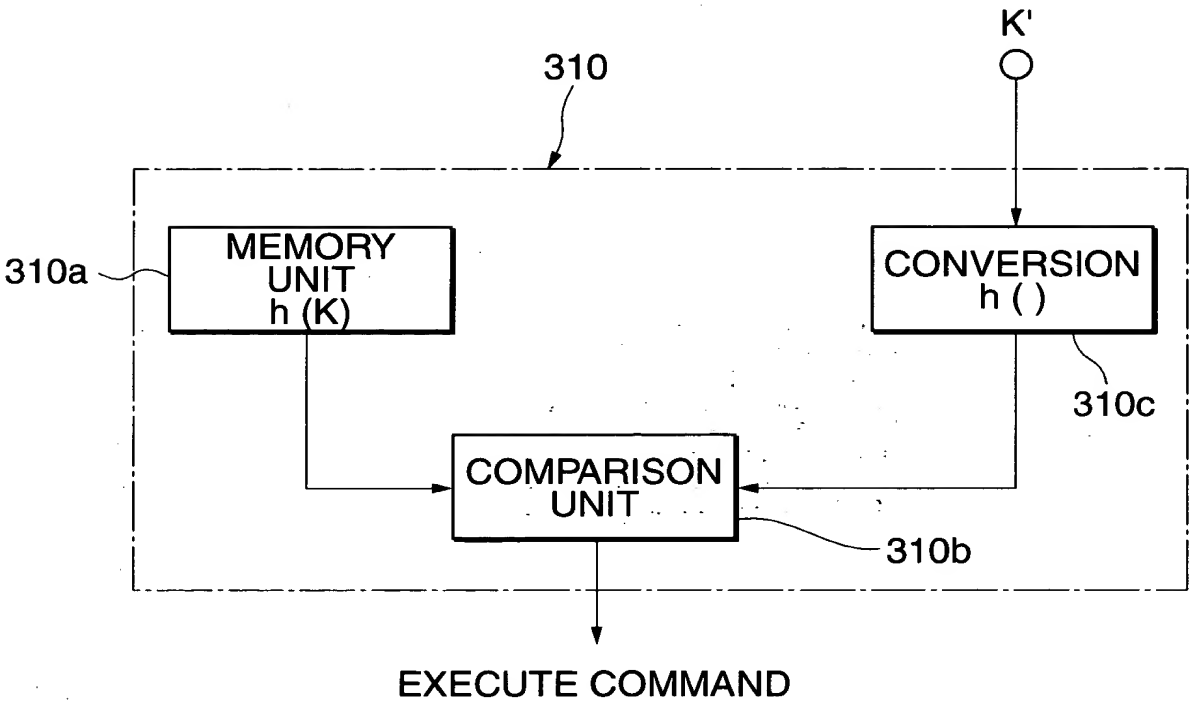

K'
310
MEMORY UNIT h (K)
310a
CONVERSION h ( )
310c
COMPARISON UNIT
310b
EXECUTE COMMAND

FIG.11

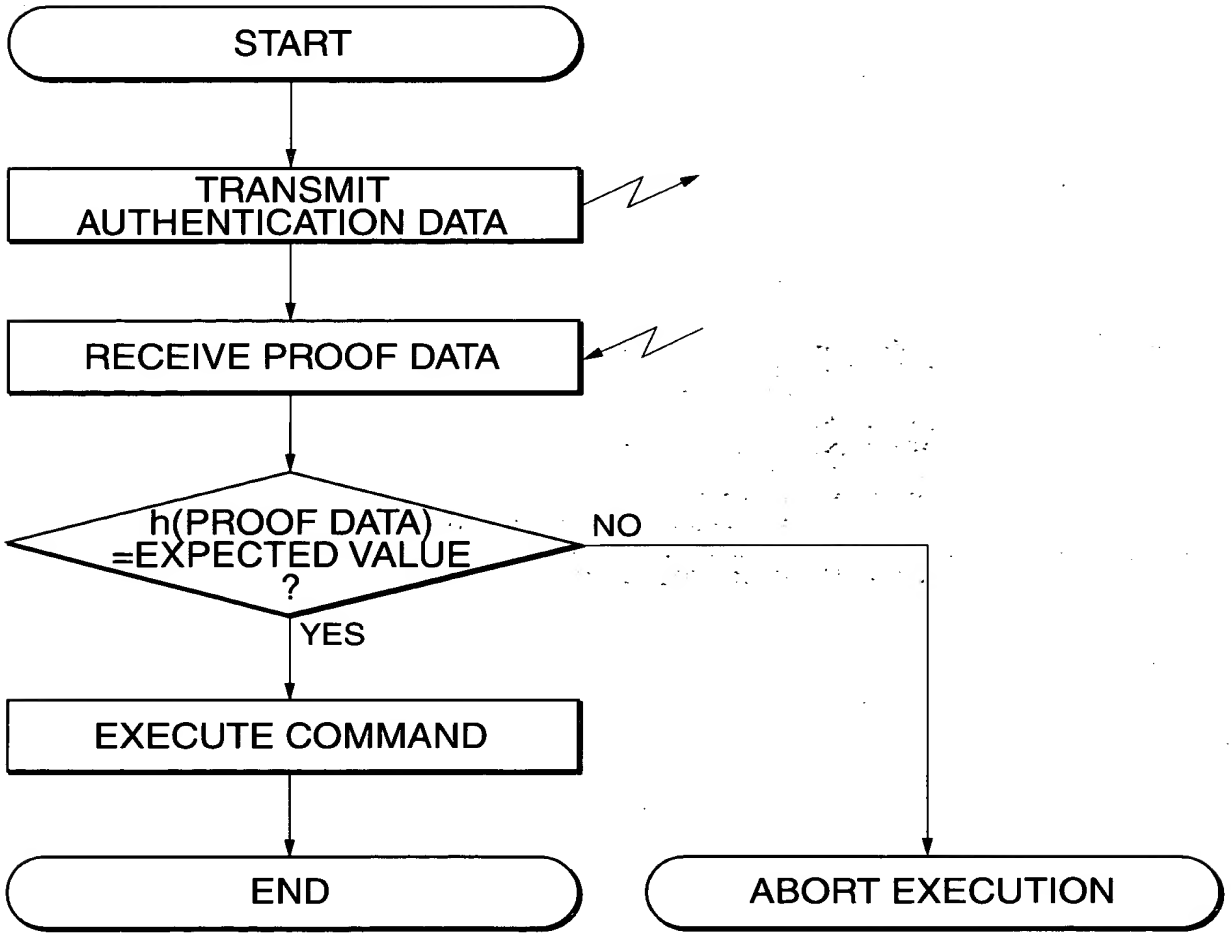

START
TRANSMIT AUTHENTICATION DATA
RECEIVE PROOF DATA
h(PROOF DATA) =EXPECTED VALUE ?
NO
YES
EXECUTE COMMAND
END
ABORT EXECUTION

FIG.12

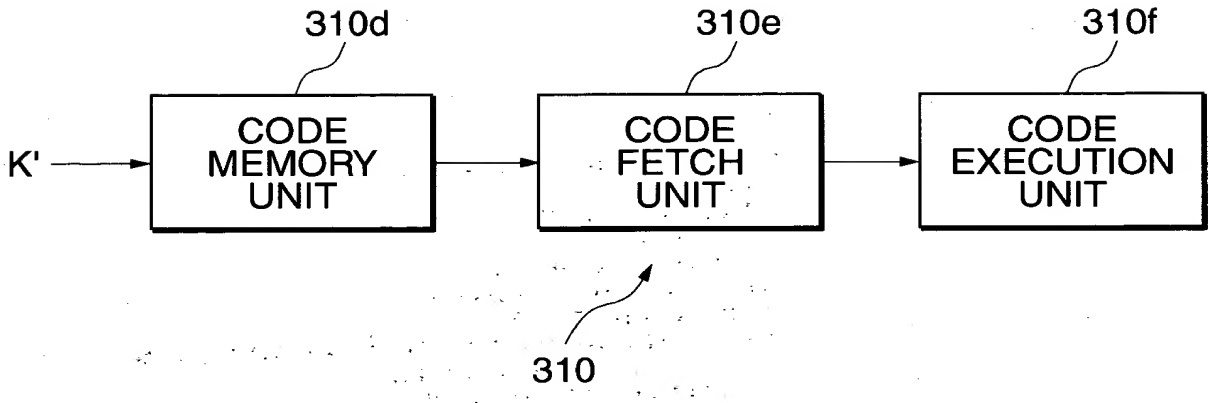

310d
310e
310f
K'
CODE MEMORY UNIT
CODE FETCH UNIT
CODE EXECUTION UNIT
310

FIG.13

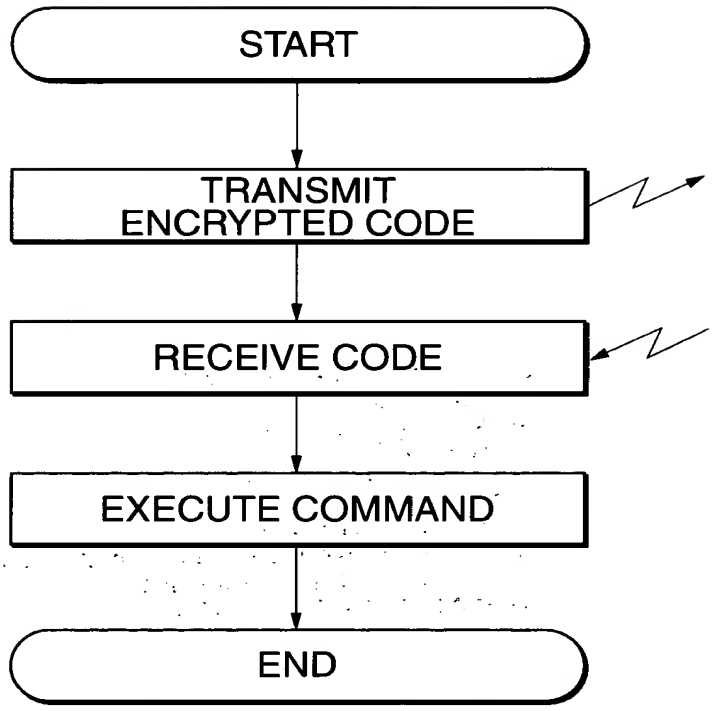

START
TRANSMIT ENCRYPTED CODE
RECEIVE CODE
EXECUTE COMMAND
END

FIG.14

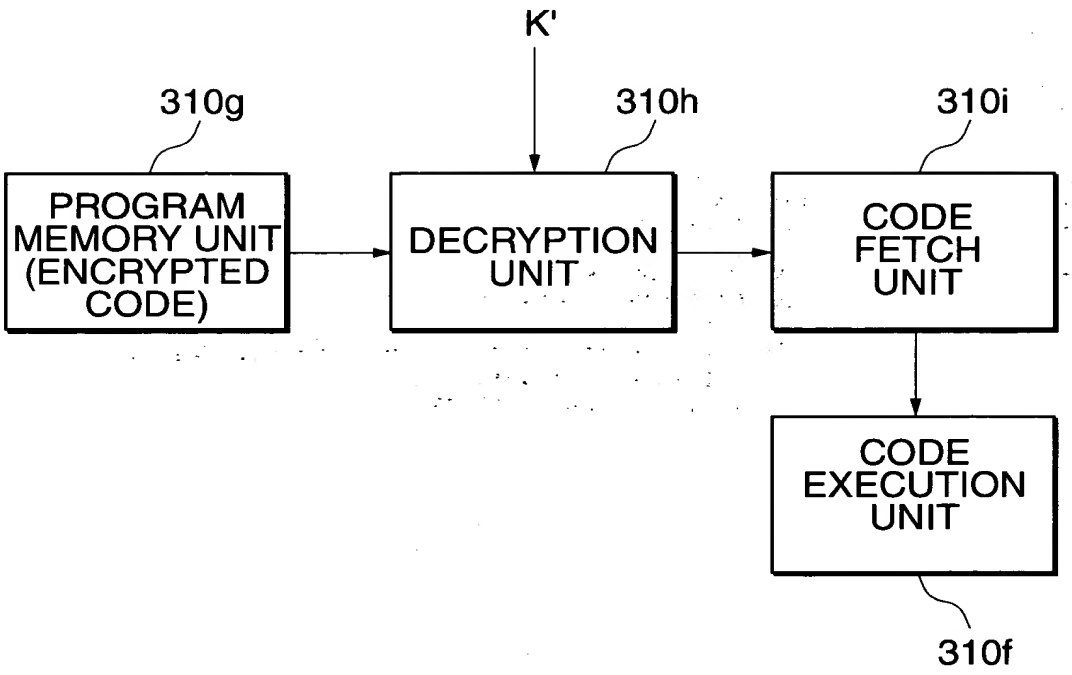

K'
310g
310h
310i
PROGRAM MEMORY UNIT (ENCRYPTED CODE)
DECRYPTION UNIT
CODE FETCH UNIT
CODE EXECUTION UNIT
310f

FIG.15

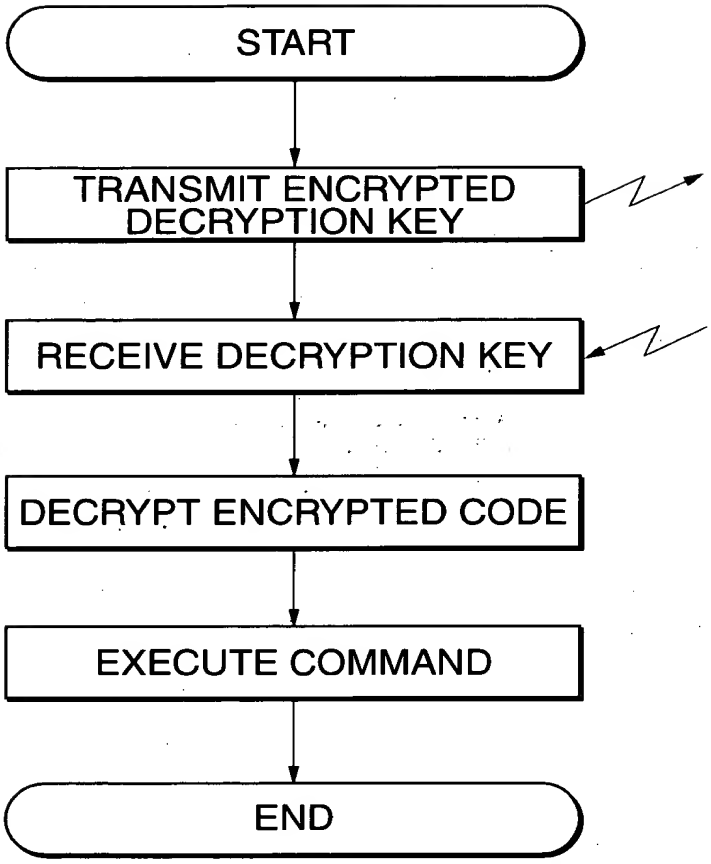

START
TRANSMIT ENCRYPTED DECRYPTION KEY
RECEIVE DECRYPTION KEY
DECRYPT ENCRYPTED CODE
EXECUTE COMMAND
END

FIG.16

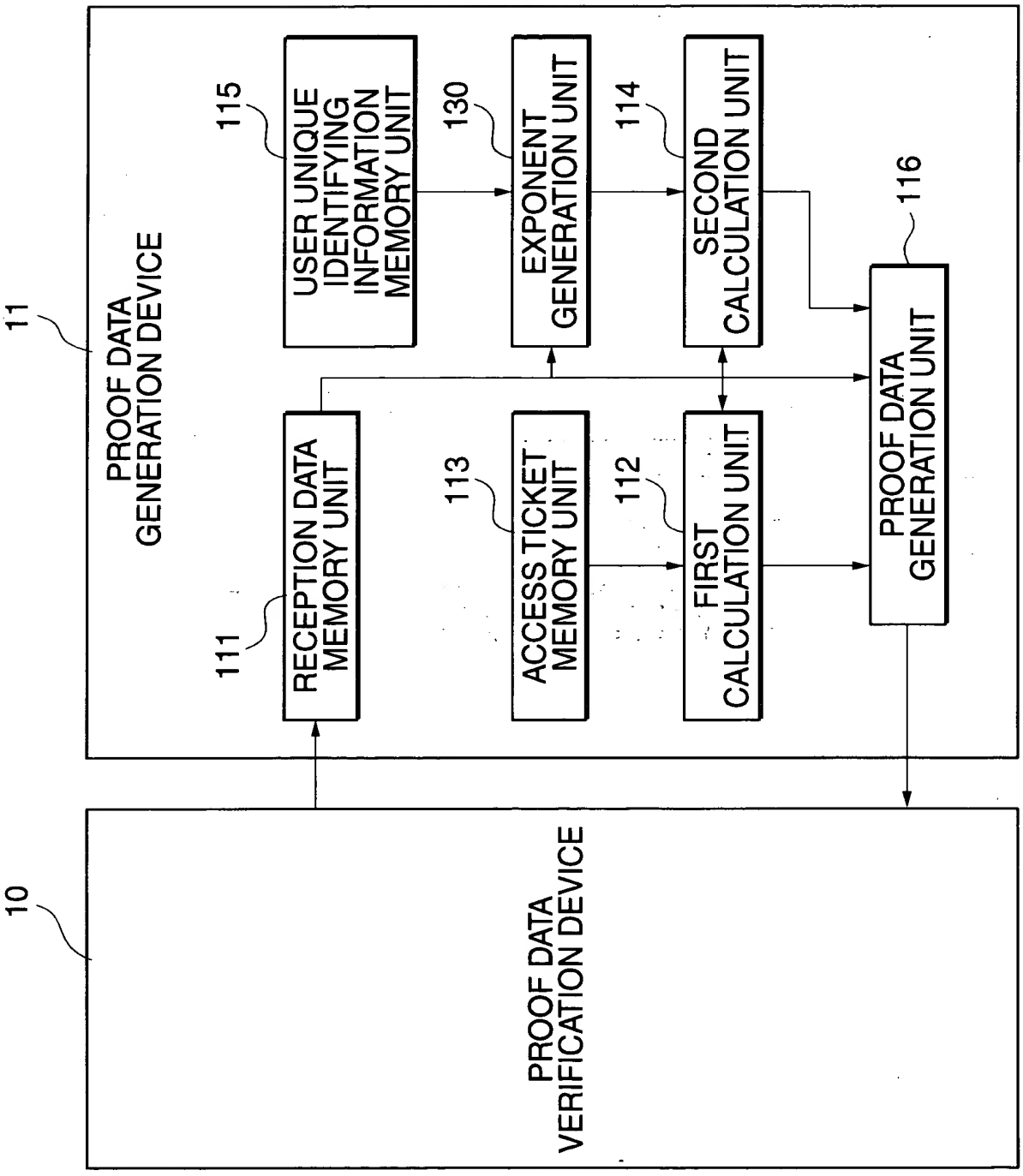

10
PROOF DATA VERIFICATION DEVICE
11
PROOF DATA GENERATION DEVICE
111
RECEPTION DATA MEMORY UNIT
113
ACCESS TICKET MEMORY UNIT
112
FIRST CALCULATION UNIT
115
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
130
EXPONENT GENERATION UNIT
114
SECOND CALCULATION UNIT
116
PROOF DATA GENERATION UNIT

FIG.17

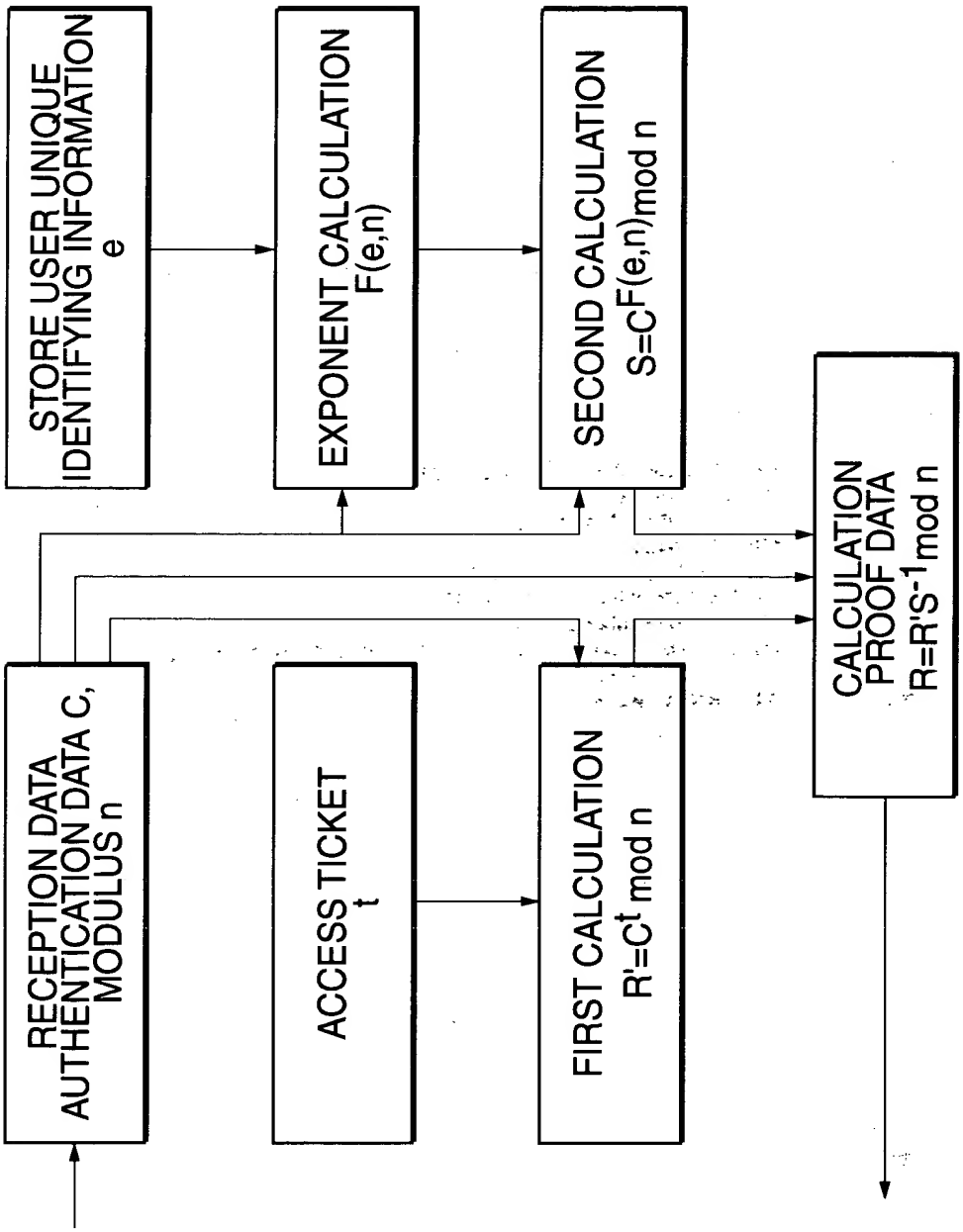
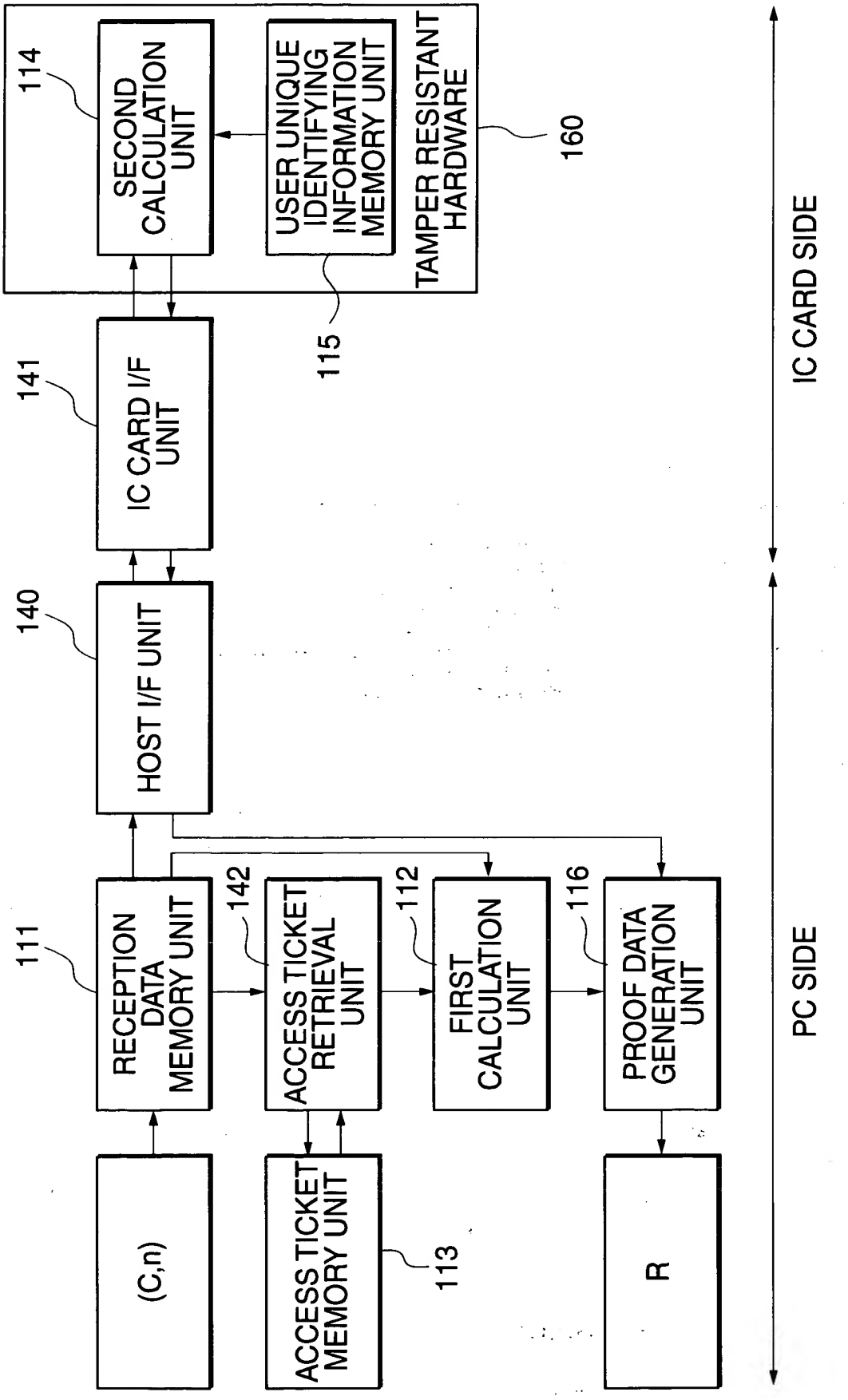

STORE USER UNIQUE IDENTIFYING INFORMATION e
EXPONENT CALCULATION F(e,n)
SECOND CALCULATION $S=C^{F(e,n)} \bmod n$
RECEPTION DATA AUTHENTICATION DATA C, MODULUS n
ACCESS TICKET t
FIRST CALCULATION $R'=C^{t} \bmod n$
CALCULATION PROOF DATA $R=R'S^{-1} \bmod n$

FIG.18


PC SIDE
IC CARD SIDE
(C,n)
RECEPTION DATA MEMORY UNIT
111
HOST I/F UNIT
140
IC CARD I/F UNIT
141
ACCESS TICKET MEMORY UNIT
113
ACCESS TICKET RETRIEVAL UNIT
142
FIRST CALCULATION UNIT
112
PROOF DATA GENERATION UNIT
116
R
TAMPER RESISTANT HARDWARE
160
SECOND CALCULATION UNIT
114
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
115

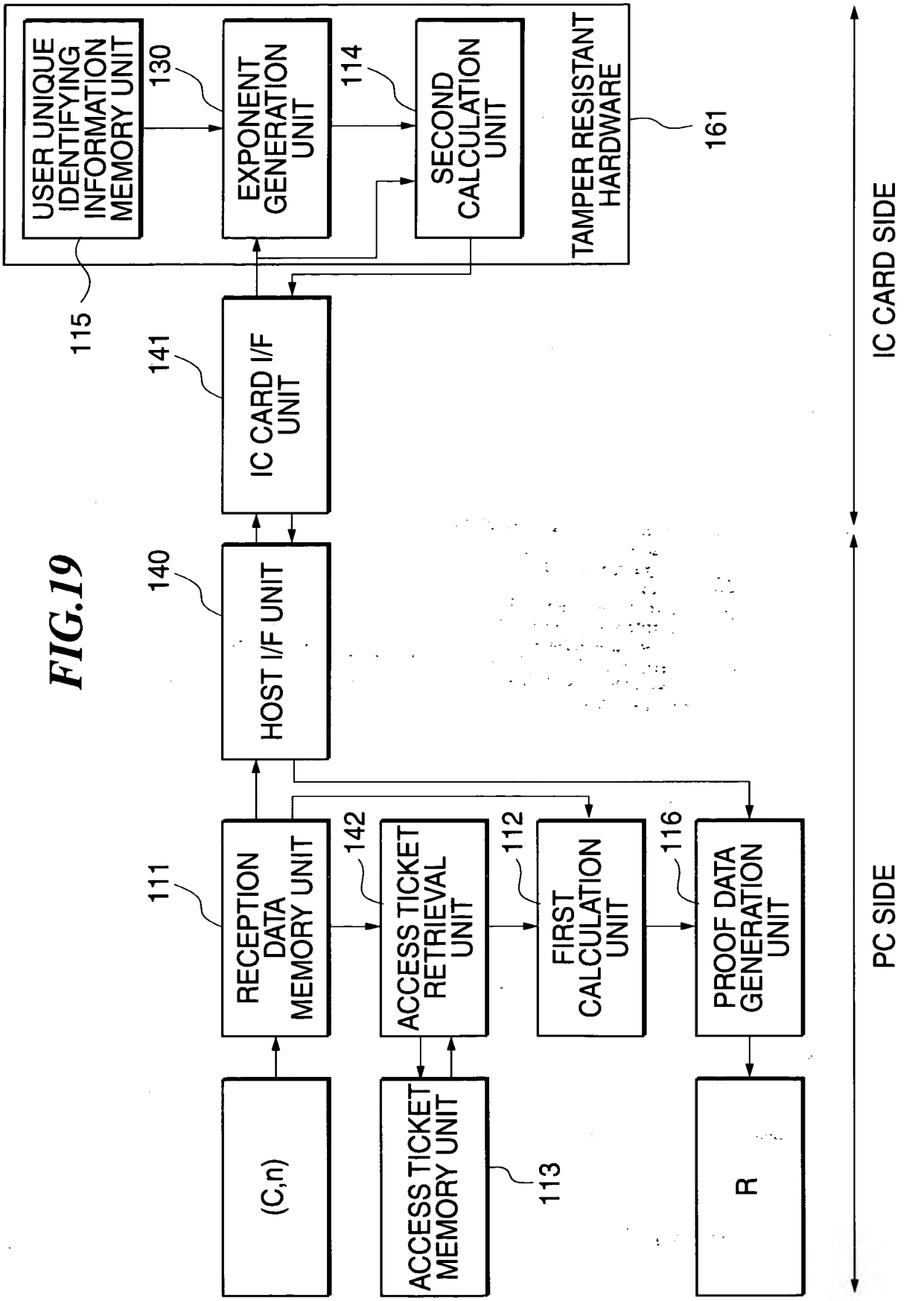

USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
130
EXPONENT GENERATION UNIT
114
SECOND CALCULATION UNIT
TAMPER RESISTANT HARDWARE
161
115
141
IC CARD I/F UNIT
140
HOST I/F UNIT
111
RECEPTION DATA MEMORY UNIT
142
ACCESS TICKET RETRIEVAL UNIT
112
FIRST CALCULATION UNIT
116
PROOF DATA GENERATION UNIT
(C,n)
ACCESS TICKET MEMORY UNIT
113
R
IC CARD SIDE
PC SIDE

FIG.19

FIG.20

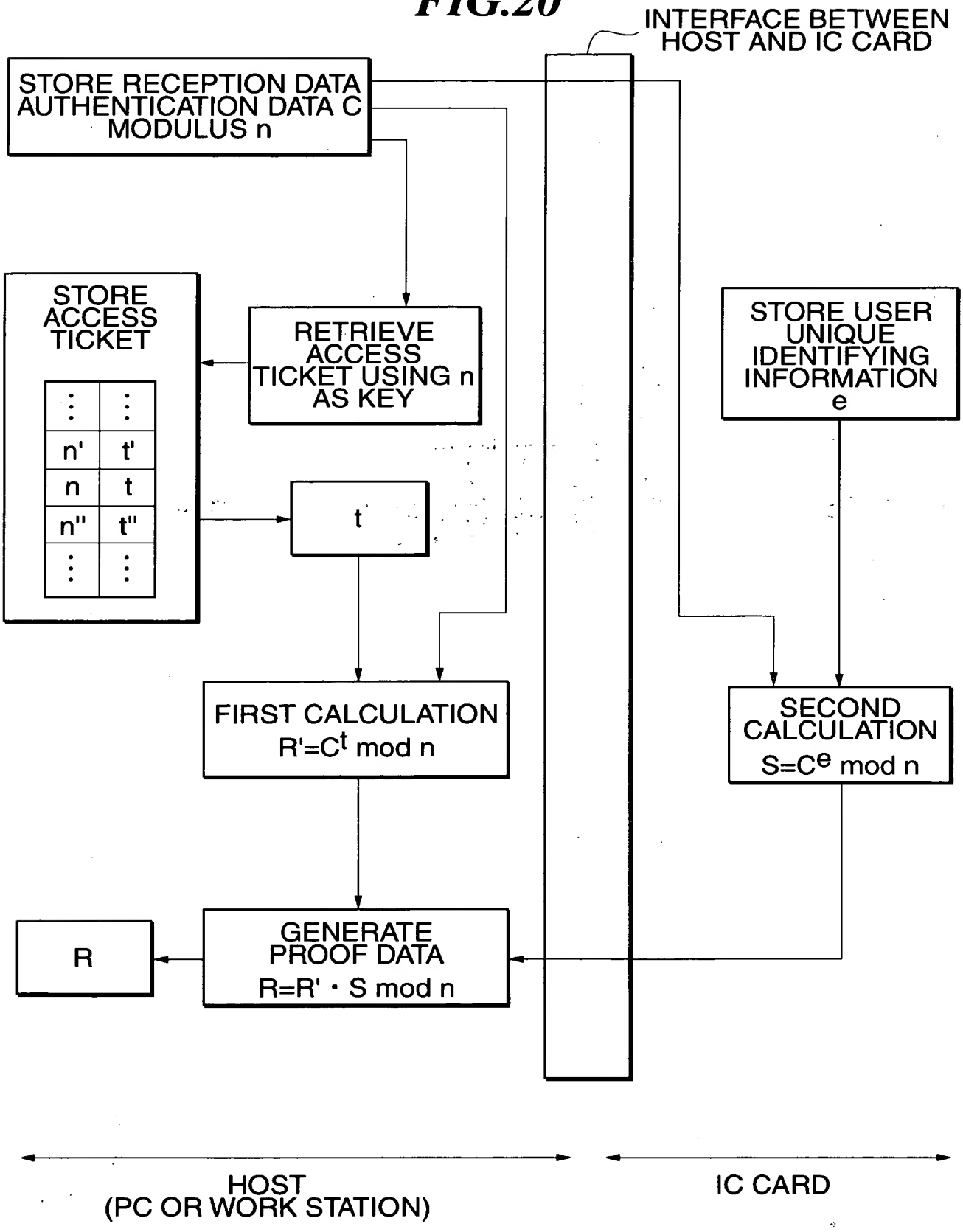

INTERFACE BETWEEN HOST AND IC CARD
STORE RECEPTION DATA AUTHENTICATION DATA C MODULUS n
STORE ACCESS TICKET
RETRIEVE ACCESS TICKET USING n AS KEY
STORE USER UNIQUE IDENTIFYING INFORMATION e
n' t'
n t
n" t"
t
FIRST CALCULATION R'=C^t mod n
SECOND CALCULATION S=C^e mod n
R
GENERATE PROOF DATA R=R' · S mod n
HOST (PC OR WORK STATION)
IC CARD

FIG.21

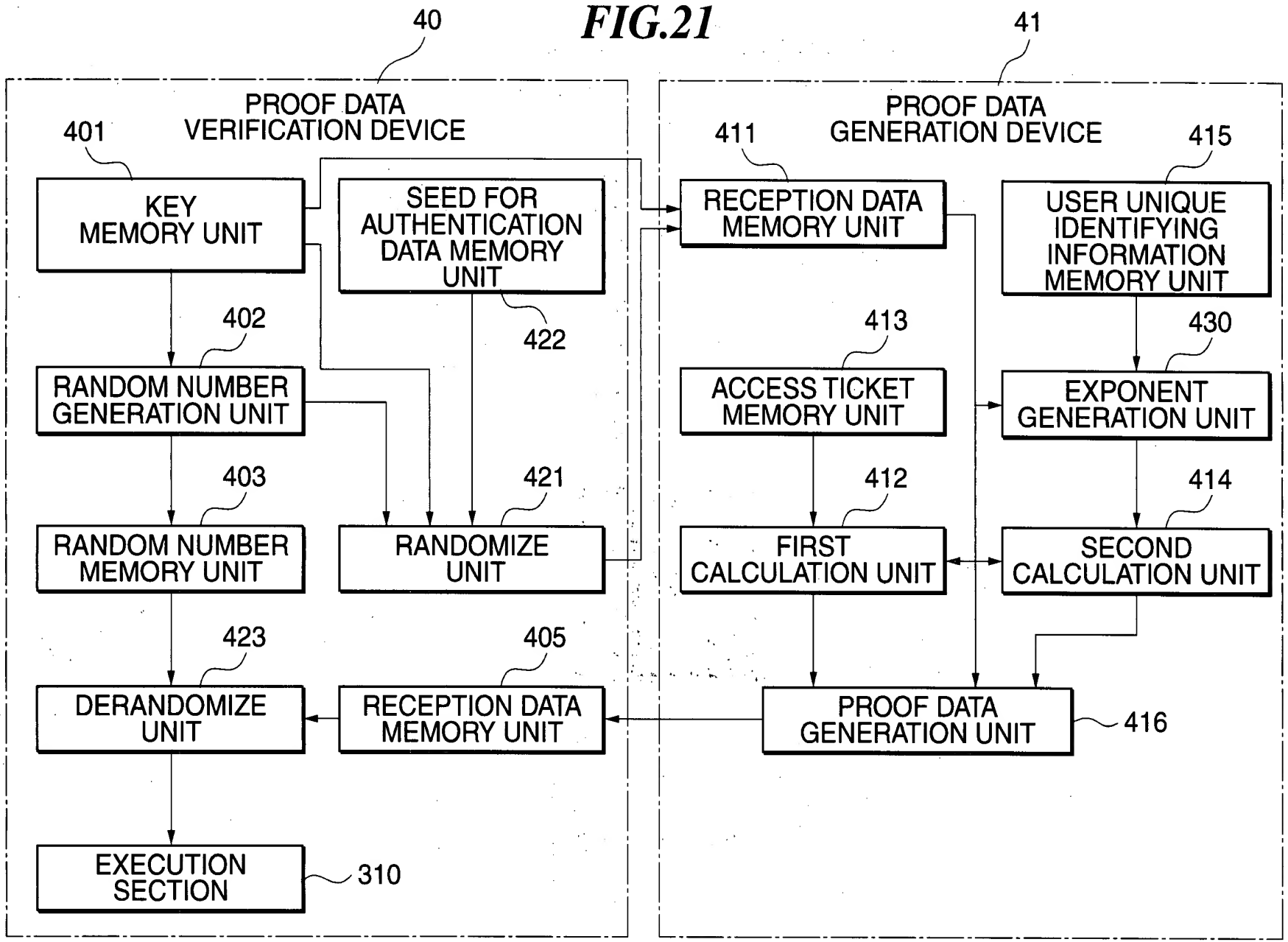

40
PROOF DATA VERIFICATION DEVICE
401
KEY MEMORY UNIT
SEED FOR AUTHENTICATION DATA MEMORY UNIT
422
402
RANDOM NUMBER GENERATION UNIT
403
RANDOM NUMBER MEMORY UNIT
421
RANDOMIZE UNIT
423
DERANDOMIZE UNIT
405
RECEPTION DATA MEMORY UNIT
EXECUTION SECTION
310
41
PROOF DATA GENERATION DEVICE
411
RECEPTION DATA MEMORY UNIT
415
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
413
ACCESS TICKET MEMORY UNIT
430
EXPONENT GENERATION UNIT
412
FIRST CALCULATION UNIT
414
SECOND CALCULATION UNIT
PROOF DATA GENERATION UNIT
416

FIG.22

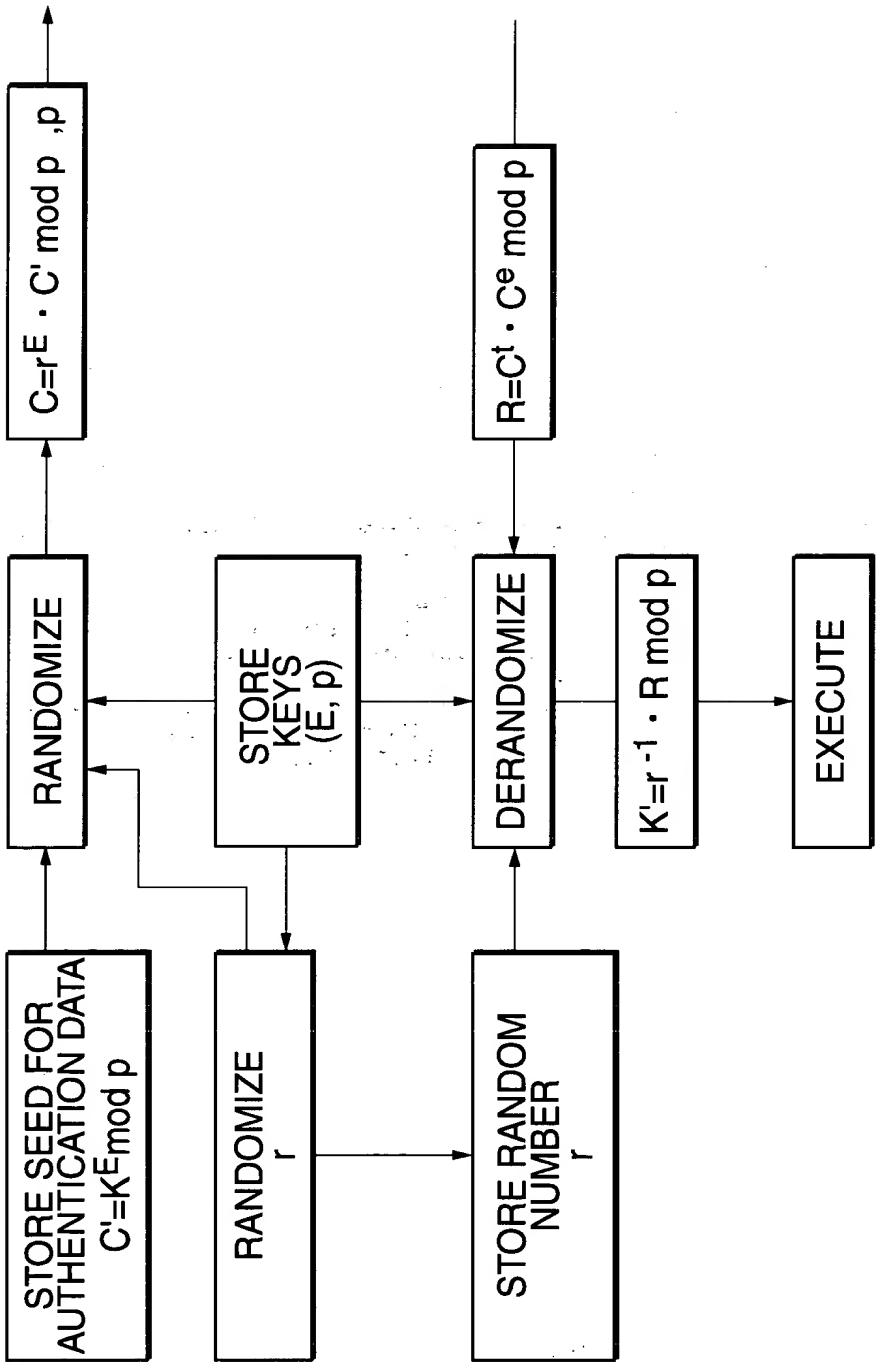

STORE SEED FOR AUTHENTICATION DATA C'=K^E mod p
RANDOMIZE
C=r^E · C' mod p ,p
RANDOMIZE r
STORE KEYS (E, p)
STORE RANDOM NUMBER r
DERANDOMIZE
R=C^t · C^e mod p
K'=r^-1 · R mod p
EXECUTE

FIG.23

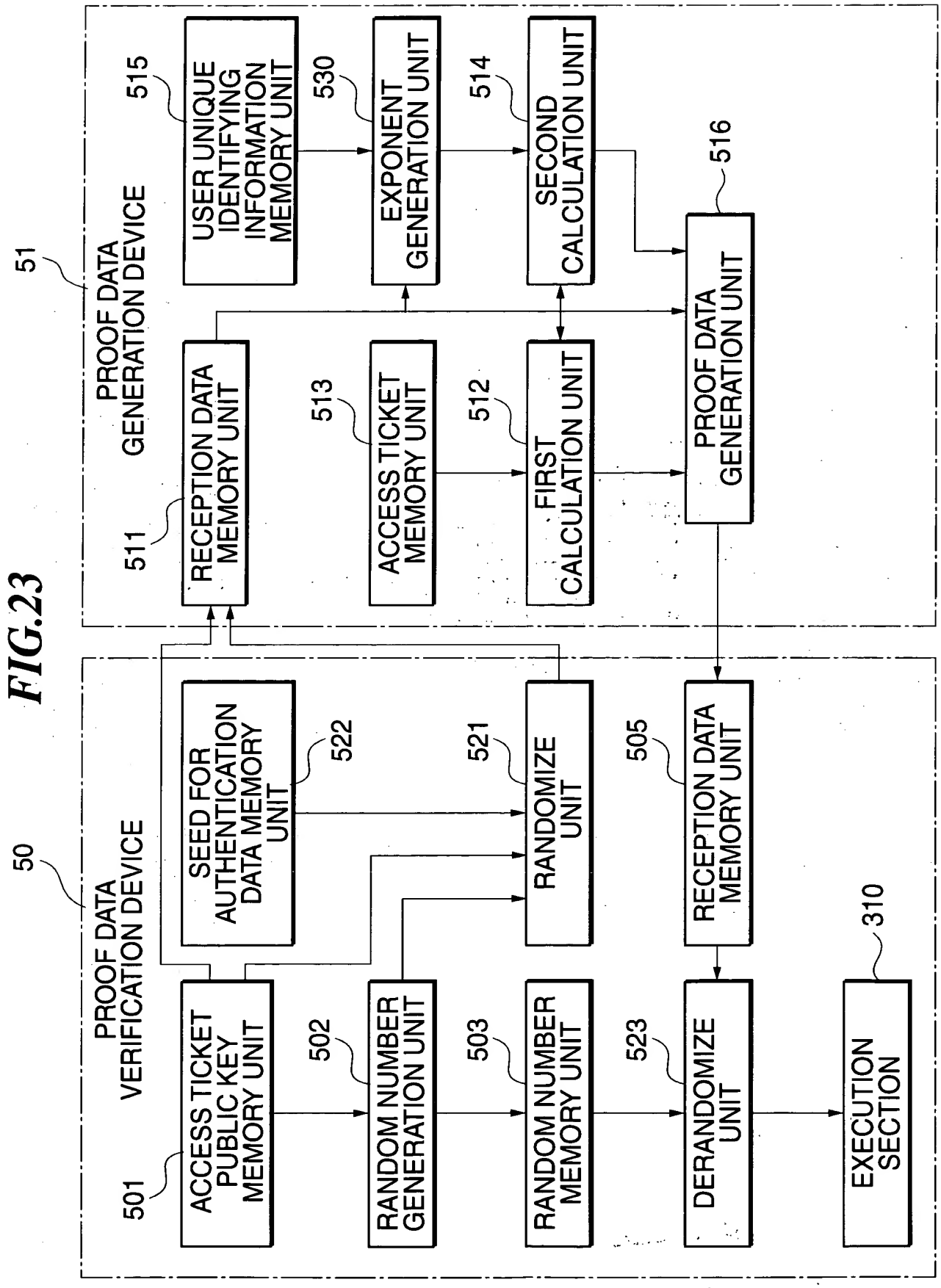

PROOF DATA VERIFICATION DEVICE
50
ACCESS TICKET PUBLIC KEY MEMORY UNIT
501
RANDOM NUMBER GENERATION UNIT
502
RANDOM NUMBER MEMORY UNIT
503
DERANDOMIZE UNIT
523
EXECUTION SECTION
310
SEED FOR AUTHENTICATION DATA MEMORY UNIT
522
RANDOMIZE UNIT
521
RECEPTION DATA MEMORY UNIT
505
PROOF DATA GENERATION DEVICE
51
RECEPTION DATA MEMORY UNIT
511
ACCESS TICKET MEMORY UNIT
513
FIRST CALCULATION UNIT
512
PROOF DATA GENERATION UNIT
516
SECOND CALCULATION UNIT
514
EXPONENT GENERATION UNIT
530
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
515

FIG.24

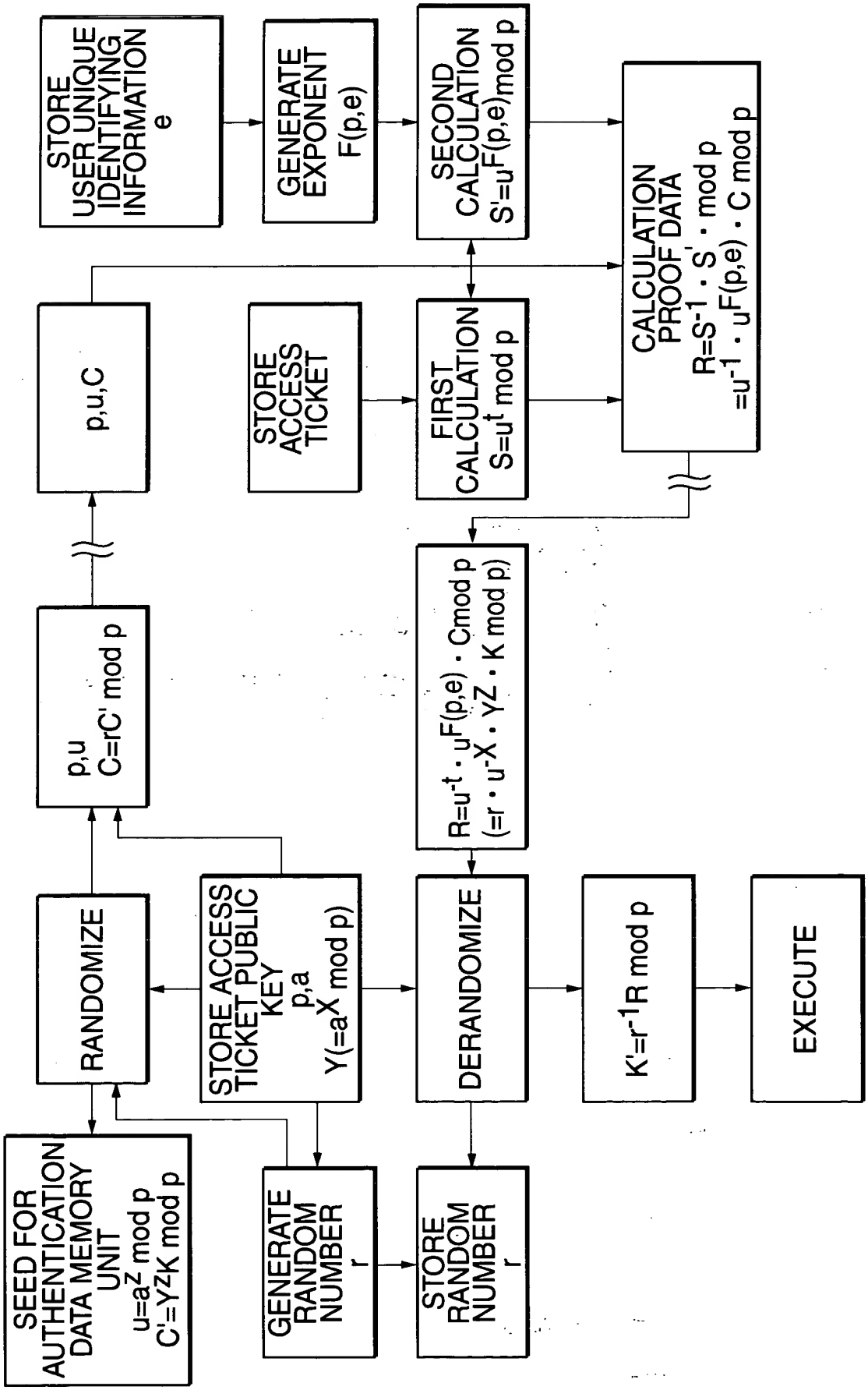

SEED FOR AUTHENTICATION DATA MEMORY UNIT
u=a^Z mod p
C'=Y^ZK mod p
RANDOMIZE
p,u
C=rC' mod p
p,u,C
STORE USER UNIQUE IDENTIFYING INFORMATION e
GENERATE EXPONENT F(p,e)
SECOND CALCULATION S'=u^F(p,e) mod p
STORE ACCESS TICKET
FIRST CALCULATION S=u^t mod p
CALCULATION PROOF DATA
R=S^-1 · S' · mod p
=u^-1 · u^F(p,e) · C mod p
STORE ACCESS TICKET PUBLIC KEY
p,a
Y(=a^X mod p)
GENERATE RANDOM NUMBER r
STORE RANDOM NUMBER r
R=u^-t · u^F(p,e) · Cmod p
(=r · u^-X · YZ · K mod p)
DERANDOMIZE
K'=r^-1R mod p
EXECUTE

FIG.25

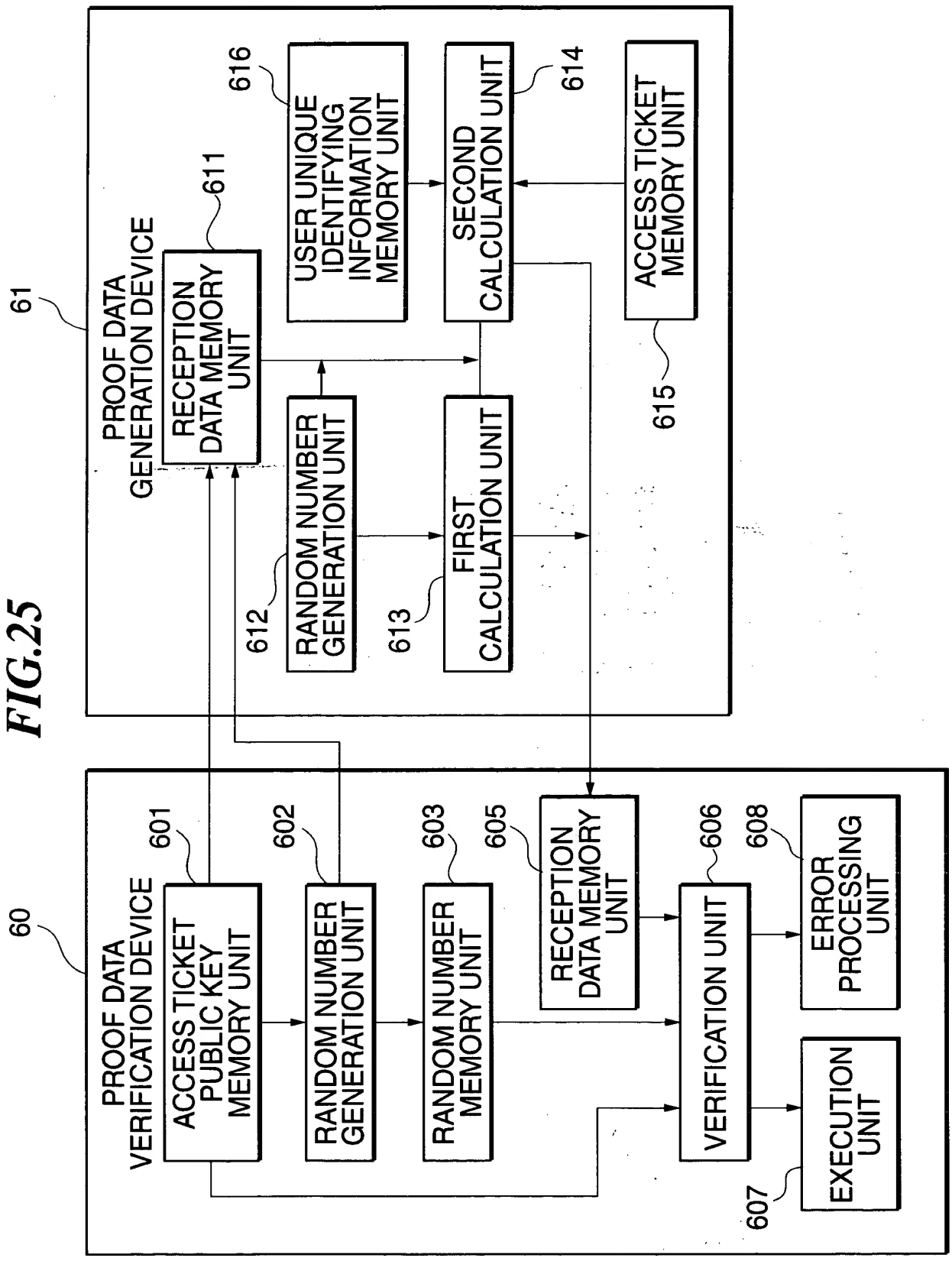

PROOF DATA GENERATION DEVICE
61
RECEPTION DATA MEMORY UNIT
611
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
616
SECOND CALCULATION UNIT
614
ACCESS TICKET MEMORY UNIT
615
RANDOM NUMBER GENERATION UNIT
612
FIRST CALCULATION UNIT
613
PROOF DATA VERIFICATION DEVICE
60
ACCESS TICKET PUBLIC KEY MEMORY UNIT
601
RANDOM NUMBER GENERATION UNIT
602
RANDOM NUMBER MEMORY UNIT
603
RECEPTION DATA MEMORY UNIT
605
VERIFICATION UNIT
606
ERROR PROCESSING UNIT
608
EXECUTION UNIT
607

FIG.26

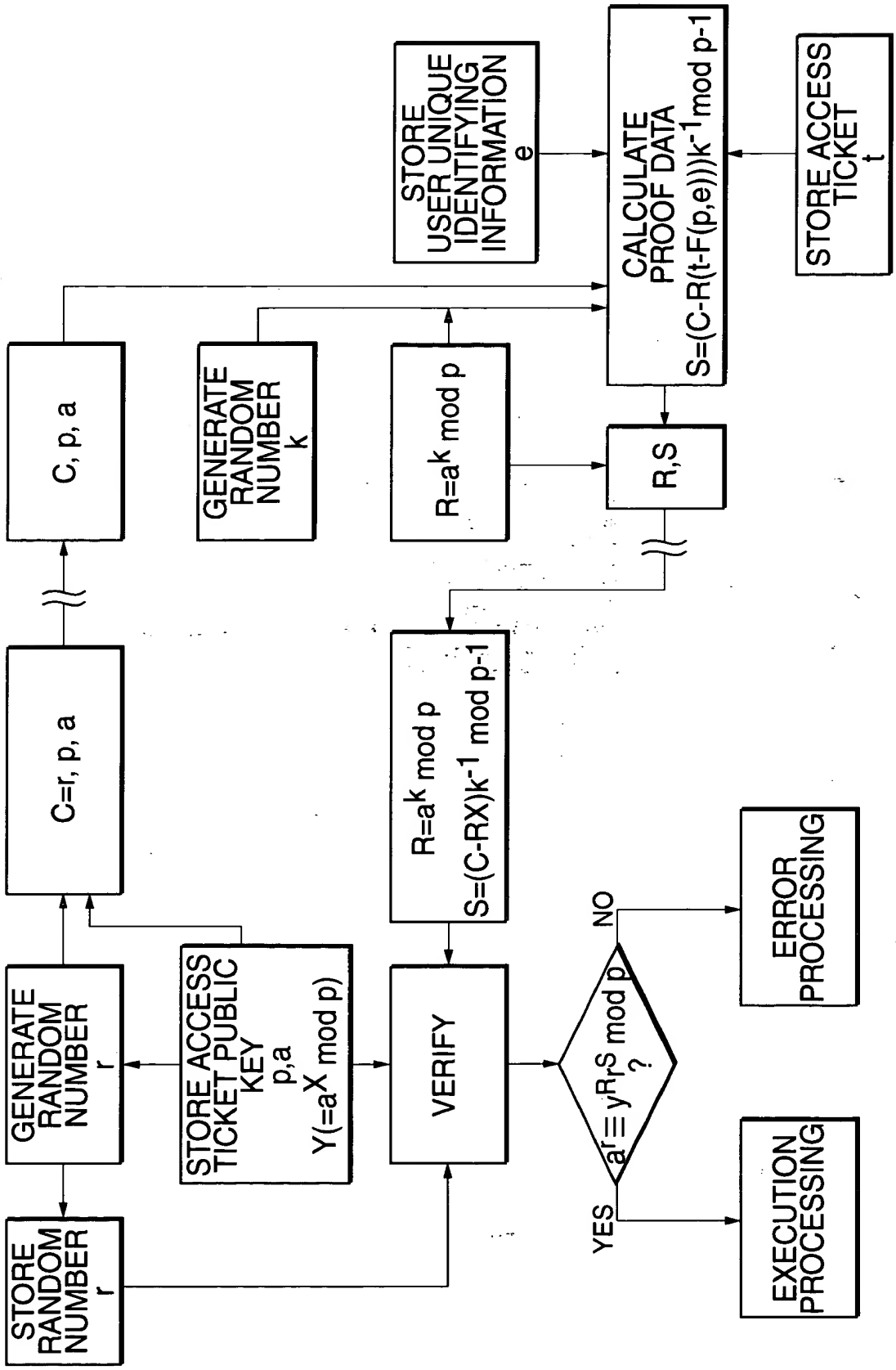

STORE RANDOM NUMBER r
GENERATE RANDOM NUMBER r
C=r, p, a
C, p, a
STORE ACCESS TICKET PUBLIC KEY p,a Y(=a^X mod p)
GENERATE RANDOM NUMBER k
R=a^k mod p
R=a^k mod p S=(C-RX)k^-1 mod p-1
R,S
STORE USER UNIQUE IDENTIFYING INFORMATION e
CALCULATE PROOF DATA S=(C-R(t-F(p,e)))k^-1 mod p-1
STORE ACCESS TICKET t
VERIFY
a^r ≡ y^R r^S mod p ?
NO
YES
ERROR PROCESSING
EXECUTION PROCESSING

FIG.27

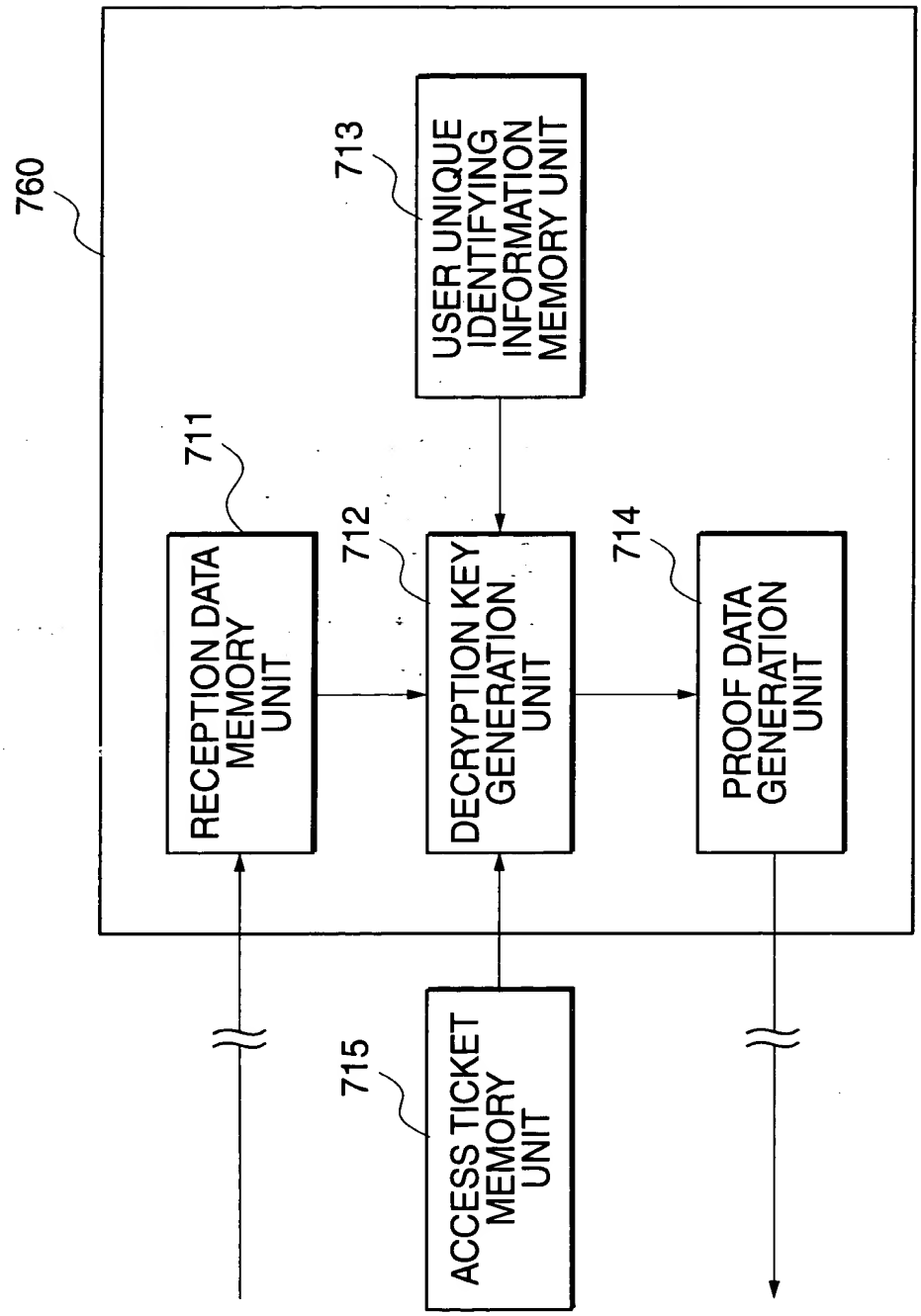
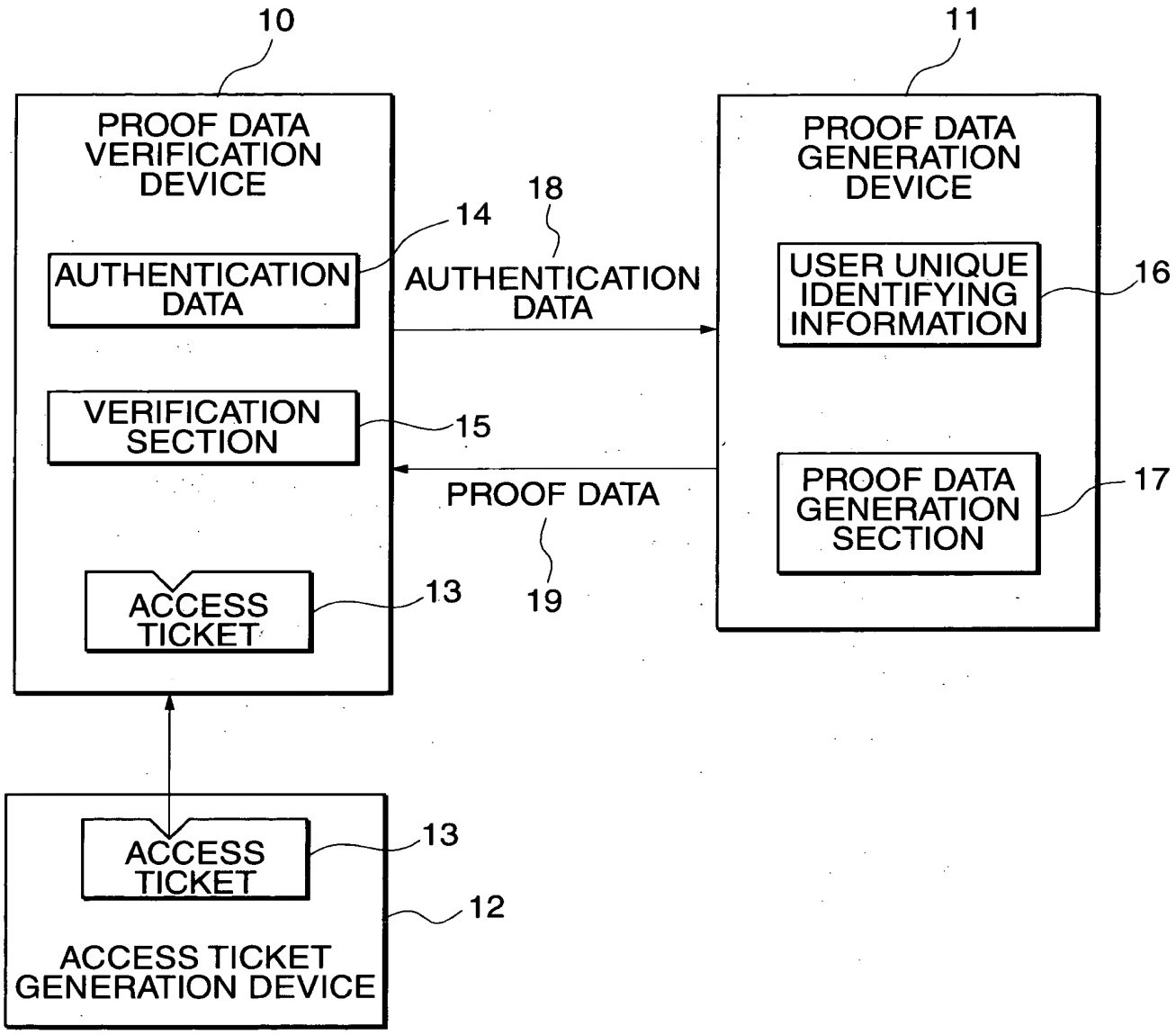

760
713
USER UNIQUE IDENTIFYING INFORMATION MEMORY UNIT
711
712
714
RECEPTION DATA MEMORY UNIT
DECRYPTION KEY GENERATION UNIT
PROOF DATA GENERATION UNIT
715
ACCESS TICKET MEMORY UNIT

FIG.28


10
PROOF DATA VERIFICATION DEVICE
AUTHENTICATION DATA
14
VERIFICATION SECTION
15
ACCESS TICKET
13
18
AUTHENTICATION DATA
PROOF DATA
19
11
PROOF DATA GENERATION DEVICE
USER UNIQUE IDENTIFYING INFORMATION
16
PROOF DATA GENERATION SECTION
17
ACCESS TICKET
13
12
ACCESS TICKET GENERATION DEVICE